REMARKS/ARGUMENTS

In the Office Action mailed December 9, 2008 (hereinafter, "Office Action"), claims 1, 3, 4, 7, 9, 12, 14 and 16-18 stand rejected under 35 U.S.C. § 112. Claims 1-18 stand rejected under 35 U.S.C. § 103. Claims 1, 8-12 and 16-18 have been amended. Claims 7 have been canceled.

Applicants respectfully respond to the Office Action.

I. Claims 1, 3, 4, 7, 9, 12, 14 and 16-18 Rejected Under 35 U.S.C § 112

Claims 1, 3, 4, 7, 9, 12, 14 and 16-18 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The detailed description including the figures and specification provide a number of details and examples that are adequate to provide support for the terms cited in the Office Action. For example, "a user input device" is clearly shown in Figure 1, along with many specific examples listed on Figure 1. The operation of an observer program is described throughout the patent application. The "user" is referred to throughout the patent application as well. Applicants respectfully request that the rejection of claims 1, 3, 4, 7, 9, 12, 14 and 16-18 be withdrawn or that further clarification be provided as to the specific issue being raised.

II. Claims 1-18 Rejected Under 35 U.S.C. § 103(a)

Claims 1-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,240,530 to Togawa (hereinafter, "Togawa") in view of U.S. Patent No. 6,006,328 to Drake (hereinafter, "Drake"). This rejection is respectfully traversed.

The factual inquiries that are relevant in the determination of obviousness are determining the scope and contents of the prior art, ascertaining the differences between the prior art and the claims in issue, resolving the level of ordinary skill in the art, and evaluating evidence of secondary consideration. KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 2007 U.S. LEXIS 4745, at **4-5 (2007) (citing Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 17-18 (1966)). As the Board of Patent Appeals and Interferences has recently confirmed, "obviousness requires a suggestion of all limitations in a claim." In re Wada and Murphy, Appeal 2007-3733 (citing CFMT, Inc. v. Yieldup

Intern. Corp., 349 F.3d 1333, 1342 (Fed. Cir. 2003)). Moreover, the analysis in support of an obviousness rejection "should be made explicit." KSR, 2007 U.S. LEXIS 4745, at **37. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." Id. (citing In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006)).

Applicants respectfully submit that the claims at issue are patentably distinct from the cited references. The cited references do not teach or suggest all of the subject matter in these claims.

Claim 1 has been amended to recite "countermeasure instructions that alter the operation of the observer program." Towaga, alone or in combination with Drake, does not teach or suggest this subject matter. Instead Towaga states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information

> processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-

> reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Claim 1 has also been amended to recite "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed." Towaga, alone or in combination with Drake, does not teach or suggest this subject matter. Instead Togawa states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information

> processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "outputting instructions . . . that prompt the user as to whether the countermeasure instructions should be executed."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "outputting instructions . . . that prompt the user as to whether the countermeasure instructions should be executed."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "outputting instructions that obtain the results and provide the results for a user and that prompt the user

as to whether the countermeasure instructions should be executed."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed."

In view of the foregoing, Applicants respectfully submit that claim 1 is patentably distinct from the cited references. Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn because Towaga, alone or in combination with Drake, does not teach or suggest all of the subject matter of claim 1.

Claims 2-15 depend either directly or indirectly from claim 1. Accordingly, Applicants respectfully request that the rejection of claims 2-15 be withdrawn.

Claim 16 has been amended to recite "means for altering the operation of the observer program; and means for outputting the results for a user and for prompting the user as to whether the countermeasure instructions should be executed." As discussed above, Towaga, alone or in combination with Drake, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 16 is allowable.

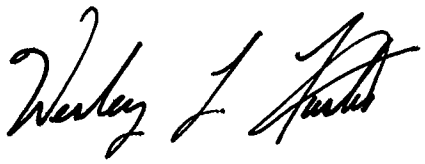
Claim 17 has been amended to recite "prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." As discussed above, Towaga, alone or in combination with Drake, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 17 is allowable.

Claim 18 has been amended to recite "prompt the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." As discussed above, Towaga, alone or in combination with Drake, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 18 is allowable.

III. Conclusion

Applicants respectfully assert that all pending claims are patentably distinct from the cited references, and request that a timely Notice of Allowance be issued in this case. If there are any remaining issues preventing allowance of the pending claims that may be clarified by telephone, the Examiner is requested to call the undersigned.

Respectfully submitted,



/Wesley L. Austin/

Wesley L. Austin
Reg. No. 42,273
Attorney for Applicant

Date: June 9, 2009

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
Salt Lake City, Utah 84101
Telephone: (801) 537-1700